REMARKS

Applicant thanks the Examiner for carefully considering this application.

Disposition of Claims

Claims 1-20 and 22-35 were pending in the present patent application. By way of this reply, claim 10 has been cancelled without prejudice or disclaimer. Accordingly, claims 1-9, 11-20 and 22-35 are pending in the present patent application. Claims 1, 17, 18, 34, and 35 are independent. The remaining claims depend, either directly or indirectly, from claims 1, 17, 18, 34, and 35.

Claim Amendments

Claims 1 and 17 have been amended to include the limitations of now-canceled dependent claim 10. Claims 11-16, 18, 19, 24, 25, 34, and 35 have been amended for clarification. No new matter has been added by way of these amendments as support for these amendments may be found, for example, in paragraphs [0030] and [0026] of the Instant Specification.

Specification Amendments

Paragraphs [0031] and [0034] of the Instant Specification have been amended to correct typographical errors. No new matter has been introduced by way of this amendment as support for this amendment may be found, for example, in Figure 4 and Figure 6.

Drawings

Applicant respectfully requests the Examiner to acknowledge whether the formal drawings filed on December 21, 2001 are acceptable.

Rejections under 35 U.S.C. §101

Claims 18-20 and 22-35 were rejected under 35 U.S.C. §101 because the claimed invention as disclosed is inoperative and therefore lacks utility. For the reasons set forth below, the rejection is respectfully traversed.

The Examiner asserts that independent claims 18, 34, and 35, teach the encryption key is hashed and stored presumably for future manipulation. The Examiner further asserts Applicant's method and apparatus does not have any use because the encryption key cannot be recovered. (*See* Office Action dated May 17, 2005 at page 4). Applicant acknowledges hash functions are one-way functions and one-way functions are "secure" in that an inverse operation does not exist. However, Applicant respectfully asserts that the encryption key is hashed and stored for future access and/or comparison in its hashed form (as needed), *not* manipulation. The invention does not contemplate retrieving the encryption key in its original form. The hashed encryption key remains hashed and is only accessed and/or compared in its hashed form. Accordingly, an inverse operation is not required to access or compare the *hashed* encryption key. Thus, contrary to the Examiner's assertion, Applicant's method and apparatus does have utility as required under 35 U.S.C. §101.

Claims 18, 34, and 35 have been amended to recite, in part, "serializing the vector to produce an encrypted serialized file and storing the encrypted serialized file in a key management system storage to persist beyond the time the key management system is active." Therefore, amended claims 18, 34 and 35 recite the use of both data and an algorithm to produce a concrete, tangible, and useful result (*e.g.*, an encrypted serial file accessible only to those with the key encryption key). Thus, Applicant respectfully asserts that claims 18-20 and 21-35 are

directed to statutory subject matter and have utility. Accordingly, withdrawal of this rejection is respectfully requested.

Rejections under 35 U.S.C. §112

Claims 18-35 stand rejected under 35 U.S.C. §112, paragraph two, as being indefinite for failing to distinctly point out and claim the subject matter of the invention. Reconsideration of the rejection is respectfully requested.

The Examiner has asserted that independent claims 18, 34, and 35, teach the encryption key is hashed and stored presumably for future manipulation. (*See* Office Action dated May 17, 2005 at page 5). Applicant acknowledges hash functions are one-way functions and one-way functions are "secure" in that an inverse operation does not exist. Applicant respectfully asserts it would be clear to one with ordinary skill in the art that the encryption key of the present invention requires no manipulation to access or compare the hashed encryption key because the encryption key remains hashed when accessed and/or compared. Thus, in direct contrast to the Examiner's assertion, no inverse operation of the hash for future manipulation is contemplated by the invention or the recited claims.

Claims 18, 34, and 35 have been amended to recite, in part, "serializing the vector to produce an encrypted serialized file and storing the encrypted serialized file in a key management system storage to persist beyond the time the key management system is active." Thus, once hashed, the encryption key is sufficiently secure to be stored as an encrypted serialized file, and is only accessible in its hashed form (*See, e.g.,* Instant Specification at [0026]). Thus, it is clear that claims 18, 34, and 35 are sufficiently definite and patentable. Claims 19-20 and 22-33 depend, either directly or indirectly, from claim 18 and are allowable for at least the same reasons. Accordingly, withdrawal of this rejection is respectfully requested.

Claims 24 and 25 also stand rejected under 35 U.S.C. §112, because the Examiner asserts that Applicant improperly refers to a "tuple" with more than two elements. (*See* Office Action dated November 24, 2004 at page 4). Claims 24 and 35 have been amended to replace the word tuple with n-tuple for clarification. Thus, it is clear that claims 24 and 25 are sufficiently definite and patentable. Accordingly, withdrawal of this rejection is respectfully requested.

Rejections under 35 U.S.C. §102

Claims 1-9 and 17 stand rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,673,316 issued to Auerbach et al. (hereinafter "Auerbach"). For the reasons set forth below, this rejection is respectfully traversed.

Independent claims 1 and 17 have been amended to include the limitations of now-canceled dependent claim 10. Amended independent claims 1 and 17 recite, in part, "a serialization module serializing data obtained from the memory, the encryption module, and the hashing module in order for the data to be stored as an encrypted serial file and persist beyond the time the key management system is active." Auerbach does not teach or suggest the serialization module as recited in the claims. In fact, Auerbach is silent regarding serialization all together. Auerbach allegedly discloses data distribution over networks such as the Internet and compression techniques. (*See* Office Action dated May 17, 2005 at page 7). However, this is not equivalent to serialization as recited in the claims. Serialization, as recited in the claims does *not* reduce storage or facilitate transmission; instead, serialization causes the data to be stored as an encrypted serial file in order to persist beyond the time the Key Management System (KMS) is active. Therefore, Auerbach does not teach or suggest all the limitations of claims 1 and 17. Thus, claims 1 and 17 are patentable over Auerbach. Claims 2-9 depend,

either directly, or indirectly, from claim 1 and are allowable for at least the same reason. Accordingly, withdrawal of this rejection is respectfully requested.

Rejections under 35 U.S.C. §103

Claims 10-16, 18-20 and 22-35 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Auerbach. By way of this reply, claim 10 has been canceled, thus the rejection is moot as to that claim. As for the remaining claims, for the reasons set forth below, this rejection is respectfully traversed.

Amended independent claim 1 is allowable for at least the same reasons argued by Applicant above for the rejection under 35 U.S.C. §102(b). Claims 11-16, which depend directly from claim 1, are allowable for at least the same reasons. Thus, Auerbach, whether considered separately or in combination, fails to teach or suggest all limitations of claims 11-16. Accordingly, withdrawal of this rejection is respectfully traversed.

The Examiner has rejected claims 18, 34, and 35 asserting that it would be obvious to one of ordinary skill to apply compression algorithms to the cryptographic envelope allegedly taught in Auerbach, to reduce storage and thereby facilitate more efficient transmission over networks such as the internet. (*See* Office Action dated May 17, 2004 at page 7). The Examiner has attempted to equate this compression algorithm to the step of serializing a vector as recited in claims 18, 34, and 35. Applicant respectfully acknowledges that serialization is the flattening of an n-dimensional object in to a one-dimensional object or "vector" and that the cryptographic envelope as taught by Auerbach is an n-dimensional object. However, serialization, as recited in claims 18, 34, and 35, does *not* reduce storage or facilitate transmission; instead, serialization causes the data to be stored as an encrypted serial file in order to persist beyond the time the Key Management System (KMS) is active. (*See* Instant Specification at [0030]). Clearly, the

compression algorithm in Auerbach does not teach or suggest serializing as recited in claims 18, 34 and 35. Claims 19, 20, and 22-33 depend, either directly or indirectly from claim 18, and are patentable for at least the same reason. Accordingly, withdrawal of this rejection is respectfully requested.

Conclusion

Applicant believes this reply is fully responsive to all outstanding issues and places this application in condition for allowance. If this belief is incorrect, or other issues arise, the Examiner is encouraged to contact the undersigned or his associates at the telephone number listed below. Please apply any charges not covered, or any credits, to Deposit Account 50-0591 (Reference Number 09469.010001).

Dated: August 10, 2005

Respectfully submitted,

By 

Robert P. Lord
Registration No.: 46,479
OSHA · LIANG LLP
1221 McKinney St., Suite 2800
Houston, Texas 77010
(713) 228-8600
(713) 228-8778 (Fax)
Attorney for Applicant

Attachment